

Timothy S. DeJong, OSB No. 940662
Email: tdejong@stollberne.com
STOLL STOLL BERNE LOKTING
& SHLACHTER P.C.
209 SW Oak Street, Suite 500
Portland, OR 97204
Telephone: (503) 227-1600
Facsimile: (503) 227-6840

Gary M. Klinger (*pro hac vice* application forthcoming)
Email: gklinger@milberg.com
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878

Attorneys for Plaintiffs

[Additional Counsel listed on signature page]

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF OREGON
PORTLAND DIVISION

M.R., an individual; on behalf of herself and
all others similarly situated,

Plaintiffs,

v.

SALEM HEALTH HOSPITALS AND
CLINICS, an Oregon nonprofit healthcare
provider,

Defendant.

Case No. 3:23-cv-01691

**CLASS ACTION ALLEGATION
COMPLAINT**

(Breach of Confidence; Violation of
Electronic Communications Privacy Act
("ECPA") 18 U.S.C. § 2511(1) et seq.
Unauthorized Interception, Use, And
Disclosure; Invasion of Privacy; Breach of
Implied Contract; Unjust Enrichment; and
Negligence)

JURY TRIAL DEMANDED

Plaintiff M.R.,¹ at all times relevant herein, has been a patient of Salem Health Hospitals and Clinics (“Salem Health” or “Defendant”), and brings this class action against Defendant in her individual capacity and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions, her counsels’ investigation, and upon information and belief as to all other matters, as follows:

1. Plaintiff brings this case to address Defendant’s unlawful practice of disclosing Plaintiff’s and Class Members’ confidential personally identifiable information (“PII”) and protected health information (“PHI”) (collectively referred to as “Private Information”) to third parties, including Meta Platforms, Inc. d/b/a Meta (“Facebook”) and Google, Inc. (“Google”), without consent, through the use of tracking software that is embedded in Defendant’s website.

2. Information about a person’s physical and mental health is among the most confidential and sensitive information in our society, and the mishandling of such information can have serious consequences, including discrimination in the workplace or denial of insurance coverage.

3. Defendant owns and controls <https://www.salemhealth.org> (“Defendant’s Website” or the “Website”), which it encourages patients to use for booking medical appointments, locating physicians and treatment facilities, communicating medical symptoms, searching medical conditions and treatment options, signing up for events and classes, and more.

¹ Plaintiff brings this action anonymously out of a desire to protect her personal health information under the Health Insurance Portability and Accountability Act of 1996 and Oregon law.

4. Included within Defendant's Website is the MyChart Patient Portal, which Defendant encourages patients to sign up for and use so that they can more conveniently book appointments and schedule visits, review their health records and test results, pay bills, communicate with service providers, request prescription refills, and complete medical forms virtually and remotely.

5. Unbeknownst to its patients, Defendant installed tracking technologies ("Tracking Tools") onto its Website, including the login page for the MyChart Portal. These Tracking Tools, including Meta Platforms, Inc.'s Tracking Pixel (the "Meta Pixel" or "Pixel") and Google, Inc.'s Google Analytics tool, track and collect communications with the Defendant via the Website and surreptitiously force the user's web browser to send those communications to undisclosed third parties, such as Facebook or Google.

6. Plaintiff and Class Members used the Website to submit information related to their past, present, or future health conditions, including, for example, searches for specific health conditions and treatment and the booking of medical appointments with a specific physician. Such Private Information would allow the third party (e.g., Facebook or Google) to know that a specific patient was seeking confidential medical care from Defendant, as well as the type of medical care being sought, such as treatment for cancer, pregnancy, or addiction.

7. The information collected and disclosed by Defendant's Tracking Tools is not anonymous. Facebook connects user data from Defendant's Website to the individual's Facebook ID (FID). The FID links the user to his/her Facebook profile, which contains detailed information about the profile owner's identity.

8. Similarly, Google "stores users' logged-in identifier on non-Google websites...in its logs ... Whenever a user logs-in on non-Google websites, whether in private browsing mode

or non-private browsing mode, the same identifier is associated with the data Google collects from the user's browsing activities on that website. Google further logs all such data (private and non-private) within the same logs and uses these data for serving personalized ads.”²

9. Simply put, the health information disclosed through the tracking technologies is personally identifiable.

10. Defendant is a healthcare entity and thus its disclosure of health and medical communications is tightly regulated. The United States Department of Health and Human Services (HHS) has established “Standards for Privacy of Individually Identifiable Health Information” (also known as the “Privacy Rule”) governing how health care providers must safeguard and protect Private Information. Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, no health care provider can disclose a person's personally identifiable protected health information to a third party without express written authorization.

11. In addition, as explained further below, HHS has specifically warned healthcare regulated entities that tracking technologies like those used by Defendant transmit personally identifying information to third parties, both on the public portion of the website and within the password-protection patient portal, and that such information should not be transmitted without a HIPAA-acceptable written authorization from patients.

² See *Brown v. Google LLC*, Case No. 4:20-cv-3664-YGR, 2023 WL 5029899 (N.D. Cal. Aug. 7, 2023) (Order denying summary judgment and citing internal evidence from Google employees). Google also connects user data to IP addresses, IP addresses have been classified by the United States Department of Health and Human Services (“HHS”) as personally identifying information. “Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates”, HHS, available at <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html> (last visited Aug. 29, 2023) (“Such PHI may include, for example, an individual's IP address . . .”).

12. The Federal Trade Commission (FTC) has also warned hospitals and other entities that “even if you are not covered by HIPAA, you still have an obligation to protect against impermissible disclosures of personal health information under the FTC Act and the FTC Health Breach Notification Rule.”

13. In addition, Oregon has a Protected Health Information Policy, Or. Rev. Stat. Ann. § 192.553, *et seq.*, which protects the “right to have protected health information of the individual safeguarded from unlawful use or disclosure.”

14. Despite these clear laws and regulations, Defendant has essentially planted a bug on patients’ web browsers that forced them to disclose their private and confidential communications with Defendant to third parties. Salem Health’s utilization of the Tracking Tools to secretly track and share with third parties its patients’ communications on its Website is the electronic equivalent of looking over the shoulder of each visitor for the entire duration of their Website interaction. Defendant did not disclose the presence of these Tracking Tools to its patients and Website users.

15. Healthcare patients simply do not anticipate or expect that their trusted healthcare provider will send personal health information or confidential medical information collected via its webpages to a hidden third party – let alone Facebook and Google, which both have a sordid history of privacy violations in pursuit of ever-increasing advertising revenue – without the patients’ consent. Neither Plaintiff nor any other Class Member signed a written authorization permitting Defendant to send their Private Information to Facebook or Google.

16. Defendant breached its statutory and common law obligations to Plaintiff and Class Members by, *inter alia*,: (i) failing to remove or disengage technology that was known and designed to share web-users’ information; (ii) failing to obtain the written consent of Plaintiff

and Class Members to disclose their Private Information to Facebook or others; (iii) failing to take steps to block the transmission of Plaintiff's and Class Members' Private Information through Tracking Tools like the Facebook Pixel or Google Analytics; (iv) failing to warn Plaintiff and Class Members; and (v) otherwise failing to design, and monitor its Website to maintain the confidentiality and integrity of patient Private Information.

17. As a result of Defendant's conduct, Plaintiff and Class Members have suffered numerous injuries, including: (i) invasion of privacy; (ii) loss of benefit of the bargain, (iii) diminution of value of their Private Information, (iv) statutory damages, and (v) the continued and ongoing risk to their Private Information.

18. Plaintiff seeks to remedy these harms and brings causes of action for (1) breach of confidence; (2) violation of the Electronics Communication Privacy Act ("ECPA") 18 U.S.C. § 2511(1) – unauthorized interception, use, and disclosure; (3) invasion of privacy (intrusion upon seclusion); (4) breach of implied contract; (5) unjust enrichment; and (6) negligence.

PARTIES

19. Plaintiff M.R. is a natural person and citizen of Oregon residing in Polk County where she intends to remain.

20. Defendant Salem Health Hospitals and Clinics is a health care provider that is incorporated in the State of Oregon as a nonprofit with a principal place of business located at 890 Oak Street, Salem, Oregon 97301. Service on Salem Health is proper at its registered agent, Cheryl Nester Wolfe, 890 Oak Street SE, Salem, Oregon 97301.

21. Salem Health is a regional health care provider to people in and around Oregon's Willamette Valley with facilities that "include Salem Hospital, West Valley Hospital in Dallas

and Salem Health clinics spread throughout the mid-Willamette Valley. Salem Health serves patients across Marion, Polk, Benton, Lincoln and Yamhill counties.”³

22. Defendant is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d and 45 C.F.R. Part 160-45 C.F.R. Part 162, and 45 C.F.R. Part 164 (HIPAA)).

JURISDICTION & VENUE

23. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this case is brought as a class action where the amount in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, is a citizen of a state different from Defendant.

24. This Court has federal question jurisdiction under 28 U.S.C. § 1331 because this Complaint alleges question of federal laws under the ECPA (18 U.S.C. § 2511, *et seq.*).

25. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and the acts and omissions giving rise to Plaintiff’s claims occurred in and emanated from this District.

26. Venue is proper under 28 U.S.C § 1391(b)(1) because Defendant’s principal place of business is in this District.

³ <https://www.salemhealth.org/about> (August 23, 2023).

COMMON FACTUAL ALLEGATIONS

A. The U.S. Department of Health and Human Services and Federal Trade Commission Have Warned about Use of Tracking Tools by Healthcare Providers

27. In January 2013, HHS issued a final rulemaking notice regarding modifications to the HIPAA privacy, security, enforcement, and breach notification rules under the Health Information Technology for Economic and Clinical Health Act (the “HITECH Act”) to “strengthen the privacy and security protection for individuals’ health information.” 78 Fed. Reg. 5566 (January 25, 2013).

28. As part of that final rulemaking, which became effective on March 26, 2013, HHS stated that, to be considered protected health information (PHI) under HIPAA, information did “not necessarily [need to] include diagnosis-specific information, such as information about the treatment of an individual.” 78 Fed. Reg. at 5598. Instead, “[i]f the information is tied to a covered entity, then it is protected health information by definition since it is indicative that the individual received health care services or benefits from the covered entity, and therefore it must be protected ... in accordance with the HIPAA rules.” *Id.*

29. In December 2022, HHS issued a bulletin (the “HHS Bulletin”) warning regulated entities like Defendant about the risks presented by the use of Tracking Tools on their websites:

Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals’ HIPAA-compliant authorizations, would constitute impermissible disclosures.***⁴

⁴ See *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), available at <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html> (last visited June 18, 2023) (emphasis added).

In other words, the HHS has expressly stated that entities like Defendant that implement the Facebook Pixel and Google Analytics and disclose patient information have violated HIPAA Rules unless those entities obtain a HIPAA-complaint authorization.

30. The HHS Bulletin further warns that:

While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, ***because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.***⁵

31. Additionally, HHS has warned healthcare providers that Protected Information is not limited exclusively to patient portals like MyChart, and thus Defendant still has an obligation to protect information on non-password protected (i.e., “unauthenticated”) webpages. Citing to the 2013 Final Rulemaking, HHS observed that “information that connects the individual to a regulated entity (i.e., that is indicative that the individual has received or will receive health care services or benefits from the covered entity)...relates to the individual’s past, present, or future health or health care or payment for care.”⁶

32. The HHS Bulletin went on to state:

Tracking technologies on a regulated entity’s unauthenticated webpage that addresses specific symptoms or health conditions, such as pregnancy or miscarriage, or that permits individuals to search for doctors or schedule appointments without entering credentials may have access to PHI in certain circumstances. ***For example, tracking technologies could collect an individual’s email address and/or IP address when the individual visits a regulated entity’s webpage to search for available appointments with a health care provider. In this example, the regulated entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply.***⁷

⁵ *Id.*

⁶ *Id.*

⁷ *Id.* (emphasis added)

33. In addition, HHS and the FTC have recently issued a letter, once again admonishing entities like Defendant to stop using Tracking Tools:

If you are a covered entity or business associate (“regulated entities”) under HIPAA, you must comply with the HIPAA Privacy, Security, and Breach Notification Rules (HIPAA Rules), with regard to protected health information (PHI) that is transmitted or maintained in electronic or any other form or medium. ***The HIPAA Rules apply when the information that a regulated entity collects through tracking technologies or discloses to third parties (e.g., tracking technology vendors) includes PHI.*** . . . Even if you are not covered by HIPAA, you still have an obligation to protect against impermissible disclosures of personal health information under the FTC Act and the FTC Health Breach Notification Rule. . . . As recent FTC enforcement actions demonstrate, it is essential to monitor data flows of health information to third parties via technologies you have integrated into your website or app. The disclosure of such information without a consumer’s authorization can, in some circumstances, violate the FTC Act as well as constitute a breach of security under the FTC’s Health Breach Notification Rule.⁸

B. Underlying Web Technology

34. To understand Defendant’s unlawful data-sharing practices, it is important first to understand basic web design and tracking tools.

35. Devices (such as computer, tablet, or smart phone) access web content through a web browser (e.g., Google’s Chrome browser, Mozilla’s Firefox browser, Apple’s Safari browser, and Microsoft’s Edge browser).

36. Every website is hosted by a computer “server” that holds the website’s contents and through which the entity in charge of the website exchanges communications with Internet users’ client devices via their web browsers.

⁸ *Re: Use of Online Tracking Technologies*, U.S. Dept. of Health & Hum. Servs. and Fed. Trade Comm’n (July 20, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf

37. Web communications consist of HTTP or HTTPS Requests and HTTP or HTTPS Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies:

- **Universal Resource Locator (“URL”):** a web address.
- **HTTP Request:** an electronic communication sent from the client device’s browser to the website’s server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL, GET Requests can also send data to the host server embedded inside the URL, and can include cookies.
- **Cookies:** a small text file that can be used to store information on the client device which can later be communicated to a server or servers. Cookies are sent with HTTP Requests from client devices to the host server. Some cookies are “third-party cookies,” which means they can store and communicate data when visiting one website to an entirely different website.
- **HTTP Response:** an electronic communication that is sent as a reply to the client device’s web browser from the host server in response to an HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data.⁹

38. Every website is comprised of Markup and “Source code.” Source code is simply a set of instructions that commands the website visitor’s browser to take certain actions when the web page first loads or when a specified event triggers the code. Source code is essentially the back of the website, and the user does not see what happens in the source code.

⁹ One browsing session may consist of hundreds or thousands of individual HTTP Requests and HTTP Responses.

39. Source code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's user. Pixels are embedded in the Source Code and instruct the Website to send a second set transmissions to the third party's servers, i.e., Facebook and Google.

40. By contrast, the Markup is the façade of the Website and what the user sees.

41. As an example, a patient's HTTP Request seeks specific information from the Defendant's Website (e.g., "Find a Doctor" page), and the HTTP Response provides the requested information in the form of "Markup," forming the webpage's content and features.

42. For example, when a patient visits www.salemhealth.org and selects the "Find a Doctor" button, the patient's browser automatically sends an HTTP Request to Defendant's web server. Defendant's web server automatically returns an HTTP Response, which loads the Markup for that particular webpage. As depicted below, the user only sees the Markup, not Defendant's Source Code or underlying HTTP Requests and Responses.

← → salemhealth.org/find-a-doctor

Contact us Pay my bill Employee Login

Salem Health
Hospitals & Clinics

Services & Resources Find a Doctor Locations Community About Careers

Search for a provider by name, location, or specialty/area of practice.

Type your search terms here

Select any combination of the options below to view matching providers.

Specialty / Area of Practice

Location

Group / Practice Name

City

Gender

Search

For referring clinics

Figure 1. The image above is a screenshot taken from the user's web browser upon visiting <https://www.salemhealth.org/find-a-doctor> (Last accessed August 10, 2023).

43. The image above displays the Markup of Defendant's Webpage. Behind the scenes, however, Tracking Tools like the Facebook Pixel and the Google Analytics are embedded in the Source code, automatically transmitting what the patient does on the webpage and effectively opening a hidden spying window into the patients' browser.¹⁰

C. Tracking Tools

44. Third parties, like Facebook and Google, offer Tracking Tools as software that advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling the interception and collection of user communications and activity on those platforms.

45. These Tracking Tools are offered to entities like Defendant for "free." In fact, however, they are bartered in exchange for Defendant's patients' data.

46. The Tracking Tools are used to gather, identify, target, and market products and services to Defendant's patients. Advertisers, such as Defendant, can track other user actions and communications and can create their own tracking parameters by customizing the software on their website.

47. When a user accesses a webpage that is hosting Tracking Tools, the user's communications with the host webpage are instantaneously and surreptitiously duplicated and sent to the third party. For example, the Facebook Pixel on Defendant's Website causes the user's web browser to instantaneously duplicate the contents of the communication with the

¹⁰ When used in the context of a screen or visual display, a "pixel" is the smallest unit in such a digital display. An image or video on a device's screen can be made up of millions of individual pixels. For example, the Facebook Pixel is a tiny image file that is so small as to be invisible to website users. It is purposefully designed and camouflaged in this manner so that website users remain unaware of it.

Website and send the duplicate from the user's browser directly to Facebook's server.

48. Google Analytics is marginally different than the Facebook Pixel, but essentially accomplishes the same goal; tracking what a user communicates to Defendant's website.¹¹

49. Notably, transmissions only occur on webpages that contain Tracking Tools.¹² Thus, Plaintiff's and Class Member's Private Information would not have been disclosed to Facebook or Google via this technology but for Defendant's decisions to install the Tracking Tools on its Website.

50. Sometimes a particularly tech-savvy user attempts to circumvent browser-based wiretap technology, so a website operator can also transmit data directly to Facebook through the use of first-party cookies called Facebook's Conversions Application Programming Interface ("CAPI"), which is a server-to-server transmission. Users cannot detect or prevent transmissions through first-party cookies.

51. CAPI is another Facebook tool that functions as a redundant measure to circumvent any ad blockers or other denials of consent by the website user by transmitting

¹¹ *Comparing Google Analytics vs Facebook Pixel*, Boltic, <https://www.boltic.io/blog/google-analytics-vsfacebookpixel#:~:text=Google%20Analytics%20is%20a%20comprehensive,time%20on%20site%2C%20and%20conversions.&text=On%20the%20other%20hand%2C%20Facebo ok,user%20actions%20on%20your%20website>. (last visited July 31, 2023)

¹² Defendant's Facebook Pixel has its own unique identifier (represented as id=4655432104470418), which can be used to identify which of Defendant's webpages contain the Facebook Pixel. Separately, "Google Analytics stores a client ID in a first-party cookie named `_ga` to distinguish unique users and their sessions on your website. Analytics doesn't store the client ID when analytics storage is disabled through Consent Mode." <https://support.google.com/analytics/answer/11593727?hl=en#:~:text=Google%20Analytics%20stores%20a%20client,is%20disabled%20through%20Consent%20Mode>. (last visited Oct. 4, 2023).

information directly from Defendant's servers to Facebook's servers.^{13, 14} Facebook markets CAPI as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results."¹⁵

52. The third parties to whom a website transmits data through Tracking Tools and associated workarounds, e.g. CAPI, do not provide any substantive Website content relating to the user's communications. Instead, these third parties are typically procured to track user data and communications for marketing purposes of the website owner (*i.e.*, to bolster profits).

53. Thus, without any knowledge, authorization, or action by a user, a website owner like Defendant can use its source code to commandeer the user's computing device, causing the device to contemporaneously and invisibly re-direct the users' communications to third parties.

D. Defendant Disclosed Plaintiff's and Class Members' Private Information to Facebook and Google Using Tracking Tools

54. In this case, Defendant employed Tracking Tools, including the Facebook Pixel and Conversions API, as well as the Google Analytics tool, to intercept, duplicate, and re-direct Plaintiffs' and Class Members' Private Information to Facebook and Google.

¹³ *What is the Facebook Conversions API and how to use it*, Realbot (last updated May 20, 2022), <https://revealbot.com/blog/facebook-conversions-api/> (last visited Jan. 24, 2023).

¹⁴ "Server events are linked to a dataset ID and are processed like events sent via the Meta Pixel.... This means that server events may be used in measurement, reporting, or optimization in a similar way as other connection channels.", <https://developers.facebook.com/docs/marketing-api/conversions-api> (last visited Jan. 27, 2023).

¹⁵ *About Conversions API*, Meta Business Help Center, <https://www.facebook.com/business/help/2041148702652965?id=818859032317965> (last visited Jan. 28, 2023).

55. Defendant's Source Code manipulates the patient's browser by secretly instructing it to duplicate the patient's communications (HTTP Requests) with Defendant and to send those communications to Facebook and Google. These transmissions occur contemporaneously, invisibly, and without the patient's knowledge.

56. Thus, without its patients' consent, Defendant has effectively used its source code to commandeer and "bug" or "tap" it patients' computing devices, allowing Facebook, Google, and other third parties to listen in on all of their communications with Defendant and thereby intercept those communications, including Private Information.

57. The Tracking Tools allow Defendant to optimize the delivery of ads, measure cross-device conversions, create custom audiences, and decrease advertising and marketing costs. However, Defendant's Website does not rely on the Tracking Tools in order to function.

58. While seeking and using Defendant's services as a medical provider, Plaintiff and Class Members communicated their Private Information to Defendant via its Website.

59. Plaintiff and Class Members were not aware that their Private Information would be shared with third parties as it was communicated to Defendant because, amongst other things, Defendant did not disclose this fact.

60. Plaintiff and Class Members never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information to third parties, nor did they intend for anyone other than Defendant to be a party to their communications (many of them highly sensitive and confidential) with Defendant.

61. Defendant's Tracking Tools sent non-public Private Information to third parties like Facebook and Google, including but not limited to Plaintiff's and Class Members': (1) status as medical patients; (2) health conditions; (3) desired medical treatment or therapies; (4) desired

locations or facilities where treatment was sought; (5) phrases and search queries (such as searches for symptoms, treatment options, or types of providers); and (6) searched and selected physicians and their specialties conducted via the general search bar.

62. Importantly, the Private Information Defendant's Tracking Tools sent to third parties included personally identifying information that allowed those third parties to connect the Private Information to a specific patient. Information sent to Facebook was sent alongside the Plaintiff's and Class Members' Facebook ID (c_user cookie or "FID"), thereby allowing individual patients' communications with Defendant, and the Private Information contained in those communications, to be linked to their unique Facebook accounts and therefore their identity.¹⁶

63. A user's FID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including location, pictures, personal interests, work history, relationship status, and other details. Because the user's Facebook ID uniquely identifies an individual's Facebook account, Facebook—or any ordinary person—can easily use the Facebook ID to locate, access, and view the user's corresponding Facebook profile quickly and easily.

64. Similarly, Google users who are logged-in to their Google accounts also have an identifier that is stored in Google's logs. Google logs a user's browsing activities on non-Google websites and uses these data for serving personalized ads.¹⁷

¹⁶ Defendant's Website track and transmit data via first-party and third-party cookies. The c_user cookie or FID is a type of third-party cookie assigned to each person who has a Facebook account, and it is comprised by a unique and persistent set of numbers.

¹⁷ *Brown v. Google LLC*, Case No. 4:20-cv-3664-YGR, FN11 (quoting Google employee deposition testimony explaining how Google tracks user data).

65. Defendant deprived Plaintiff and Class Members of their privacy rights when it: (1) implemented Tracking Tools that surreptitiously tracked, recorded, and disclosed Plaintiff's and other online patients' confidential communications and Private Information; (2) disclosed patients' protected information to unauthorized third parties; and (3) undertook this pattern of conduct without notifying Plaintiff or Class Members and without obtaining their express written consent.

66. By installing and implementing both Facebook tools and Google Analytics, Defendant caused Plaintiff's and Class Member's communications to be intercepted by and/or disclosed to Facebook and Google and for those communications to be personally identifiable.

67. As explained below, these unlawful transmissions are initiated by Defendant's source code concurrent with communications made via certain webpages.

E. Defendant's Tracking Tools Disseminate Patient Information Via Its Website

68. An example illustrates the point. If a patient uses the Website to find a physician, Defendant's Website directs them to communicate Private Information, including desired physician name, location, and specialty/area of practice. Unbeknownst to the patient, this communication is sent to Facebook and other third party entities via Defendant's Pixel, including the terms searched in the search bar and the filters they select.

69. In the example below, the user navigated to the "Find a Doctor" page in Defendant's Website where the user is prompted by Defendant's Website to find a doctor by inputting personal information regarding their medical status, including desired specialty, or by using the search bar to search applicable terms:

Contact us Pay my bill Employee Login MyChart Login

Salem Health
Hospitals & Clinics

Search

Services & Resources Find a Doctor Locations Community About

Search for a provider by name, location, or specialty/area of practice.

Type your search terms here

Select any combination of the options below to view matching providers.

Specialty / Area of Practice

Location

Group / Practice Name

..

Figure 2. Screenshot taken from salemhealth.org as the user searches for a specialist and communicates information via the search bar and filtering tools.

70. In this instance, the user typed the desired specialty and zip code into the respective search boxes.

71. Unbeknownst to ordinary patients, this particular webpage—which is undoubtedly used to communicate Private Information for the purpose of seeking medical treatment—contains Defendant’s Tracking Tools. The image below shows the “behind the scenes” portion of the website that is invisible to ordinary users:

```

• method: GET
• url: https://www.facebook.com/tr/?id=4655432104470418&ev=PageView&dl=https://saalemhealth.org/find-a-doctor/Details/7f5846aa-6f29-4bcb-bb18-8e8233808a13/&rl=https://saalemhealth.org/find-a-doctor&if=false&ts=1670479774246&sw=1366&sh=768&v=2.9.89&r=stable&ec=0&co=30&fbp=fb.1.1670479633426.1786109590&it=1670479773978&coo=false&rqm=GET
• httpVersion: http/1.1
• headers:
  [{"name": "authority", "value": "www.facebook.com"}, {"name": "method", "value": "GET"}, {"name": "path", "value": "/tr/?id=4655432104470418&ev=PageView&dl=https%3A%2F%2Fsaalemhealth.org%2Ffind-a-doctor%2FDetails%2F7f5846aa-6f29-4bcb-bb18-8e8233808a13%2F&rl=https%3A%2F%2Fsaalemhealth.org%2Ffind-a-doctor&if=false&ts=1670479774246&sw=1366&sh=768&v=2.9.89&r=stable&ec=0&co=30&fbp=fb.1.1670479633426.1786109590&it=1670479773978&coo=false&rqm=GET&dt=jzc5o29vw5oi2ecaj4m"}, {"name": "scheme", "value": "https"}, {"name": "accept", "value": "image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8"}, {"name": "accept-encoding", "value": "gzip, deflate, br"}, {"name": "accept-language", "value": "en-US,en;q=0.9"}, {"name": "cookie", "value": "sb=ewMyYqATMfIs-sx4Y6lmikwj; datr=ewMyYtQzmmMstZpZmB22bB2u; locale=en_US; c_user=100011152182075; xs=32%3AKXXdrGmNjy5DIA%3A2%3A1670391700%3A-1%3A5353%3A%3AAcWtZrvS4h5XhmrRIA2sq0yWxURAUoqIN3M8ykUWeA; fi=0iDdg8Y6H3RcIXfGWAWUGmgm47tr4rYHAvIH6mSpWuIkBjkXVj.f8.AAA.0.0.BjkXVj.AWUDdZomD-S"}, {"name": "referrer", "value": "https://saalemhealth.org/"}, {"name": "sec-ch-ua", "value": "\"Not? A_Brand\";v=\"8\""}, {"name": "sec-ch-ua-mobile", "value": "?0"}, {"name": "sec-ch-ua-platform", "value": "\"Windows\""}, {"name": "sec-fetch-dest", "value": "image"}, {"name": "sec-fetch-mode", "value": "no-cors"}, {"name": "sec-fetch-site", "value": "cross-site"}, {"name": "user-agent", "value": "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36"}]

```

Figure 3. Screenshot showing network activity occurring during a GET request when a user searches for a specialist on salemhealth.org.

72. Thus, without alerting the user, Defendant's Pixel sends the communications the user made via the webpage to Facebook, and the images below confirm that the communications Defendant sends to Facebook contain the user's Private Information.

73. As seen above, the first line of highlighted text, "id=4655432104470418" refers to Defendant's Pixel ID and confirms that Defendant has downloaded the Pixel into its Source Code for this particular webpage.

74. On the same line of text, "ev= PageView," identifies and categorizes which actions the user took on the webpage ("ev=" is an abbreviation for event, and "PageView" is the type of event). Thus, this identifies the user as having navigated to the Website page.

75. The additional lines of highlighted text show Defendant has disclosed to Facebook that the user: (1) is a patient seeking medical care from Defendant via <https://salemhealth.org>; (2) a patient seeking a physician for medical care via Salem Health.

- **method:** GET
- **url:** [https://www.facebook.com/tr/?id=4655432104470418&ev=Microdata&dl=https://salemhealth.org/find-a-doctor/Details/7f5846aa-6f29-4bcb-bb18-8e8233808a13&rl=https://salemhealth.org/find-a-doctor&if=false&ts=1670479774750&cd\[DataLayer\]=\[\]&cd\[Meta\]={\"title\":\"Find a doctor | Salem Health n\", \"meta:description\":\"Salem Health providers by name, location, or specialty. Our team is here for you.\"}&cd\[OpenGraph\]={\"og:title\":\"Find a doctor | Salem Health\", \"og:description\":\"Salem Health providers by name, location, or specialty. Our team is here for you.\"}, \"og:image\":\"https://salemhealth.org/images/default-source/default-album/adobestock_296904883.jpeg?sfvrsn=b007ddc4_0\", \"og:url\":\"https://salemhealth.org/find-a-doctor\", \"og:type\":\"website\", \"og:site_name\":\"SalemHealth\"}&cd\[Schema.org\]=\[\]&cd\[JSON-LD\]=\[\]&sw=1366&sh=768&v=2.9.89&r=stable&ec=1&o=30&fp=fb.1.1670479633426.1786109590&it=1670479773978&coo=false&es=automatic&tm=3&rqm=GET](https://www.facebook.com/tr/?id=4655432104470418&ev=Microdata&dl=https://salemhealth.org/find-a-doctor/Details/7f5846aa-6f29-4bcb-bb18-8e8233808a13&rl=https://salemhealth.org/find-a-doctor&if=false&ts=1670479774750&cd[DataLayer]=[]&cd[Meta]={\)
- **http Version:** http:1.1
- **headers:**

```
{\"name\":\"authority\",\"value\":\"www.facebook.com\"},{\"name\":\"method\",\"value\":\"GET\"},{\"name\":\"path\",\"value\":\"/tr/?id=4655432104470418&ev=Microdata&dl=https://salemhealth.org/find-a-doctor/Details/7f5846aa-6f29-4bcb-bb18-8e8233808a13&rl=https://salemhealth.org/find-a-doctor&if=false&ts=1670479774750&cd[DataLayer]=[]&cd[Meta]={\"title\":\"Find a doctor | Salem Health n\", \"meta:description\":\"Salem Health providers by name, location, or specialty. Our team is here for you.\"}&cd[OpenGraph]={\"og:title\":\"Find a doctor | Salem Health\", \"og:description\":\"Salem Health providers by name, location, or specialty. Our team is here for you.\"}, \"og:image\":\"https://salemhealth.org/images/default-source/default-album/adobestock_296904883.jpeg?sfvrsn=b007ddc4_0\", \"og:url\":\"https://salemhealth.org/find-a-doctor\", \"og:type\":\"website\", \"og:site_name\":\"SalemHealth\"}&cd[Schema.org]=[]&cd[JSON-LD]=[]&sw=1366&sh=768&v=2.9.89&r=stable&ec=1&o=30&fp=fb.1.1670479633426.1786109590&it=1670479773978&coo=false&es=automatic&tm=3&rqm=GET&dt=tjfdj5guy94go3v\"},{\"name\":\"scheme\",\"value\":\"https\"},{\"name\":\"accept\",\"value\":\"image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\"},{\"name\":\"accept-encoding\",\"value\":\"gzip, deflate, br\"},{\"name\":\"accept-language\",\"value\":\"en-US,en;q=0.9\"},{\"name\":\"cookie\",\"value\":\"sb=ewMyYqATmfls-sx4Y6lmikvj; datr=ewMyYtQzmmMstZpZmB22bB2u; locale=en_US; c_user=5113293263AKXXdrGmNyy5DIA63A2963A167039170093A-1963A5353363A3AAcWtZrvS4h5XhmrRIA2sq0yWxURAUoqIN3M8ykUWeA; fr=0tDdg8Y6H3RcIXfGWAUUGmgn47r4rYHAvIH6mSpWu1k BjkXVj.f8.AAA.0.0 BjkXVj.AWUDdZomD-S\"},{\"name\":\"referrer\",\"value\":\"https://salemhealth.org\"},{\"name\":\"sec-ch-ua\",\"value\":\"NotA_Brand\",\"v\":\"8\", \"Chromium\",\"v\":\"108\", \"Google Chrome\",\"v\":\"108\"},{\"name\":\"sec-ch-ua-mobile\",\"value\":\"?0\"},{\"name\":\"sec-ch-ua-platform\",\"value\":\"\"Windows\"\"},{\"name\":\"sec-fetch-dest\",\"value\":\"image\"},{\"name\":\"sec-fetch-mode\",\"value\":\"no-cors\"},{\"name\":\"sec-fetch-site\",\"value\":\"cross-site\"},{\"name\":\"user-agent\",\"value\":\"Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36\"}]
```

Figure 4. Same screenshot as Figure 3 with different highlights for emphasis.

76. Finally, the highlighted text ("GET") demonstrates that Defendant's Pixel sent the user's communications, and the Private Information contained therein, alongside the user's

Facebook ID (c_user ID), thereby allowing the user's communications and actions on the website to be linked to their specific Facebook profile.

77. The image demonstrates that the user’s Facebook ID (highlighted as “c_user=” in the image above) was sent alongside the other data.¹⁸

78. In each of the examples above, the user's website activity and the contents of the user's communications are sent to Facebook alongside their personally identifiable information. Several different methods allow marketers and third-parties to identify individual website users, but the examples above demonstrate what happens when the website user is logged into Facebook on their web browser or device. When this happens, the website user's identity is revealed via third-party cookies that work in conjunction with the Pixel. For example, the Pixel transmits the user's c_user cookie, which contains that user's unencrypted Facebook ID, and allows Facebook to link the user's online communications and interactions to their individual Facebook profile.

79. Facebook receives at least six cookies when Defendant's website transmits information via the Pixel:

• cookies:

Figure 5. Screenshot of network analysis showing cookies sent to Facebook when a user visits salemhealth.org.

¹⁸ The user's Facebook ID is represented as the c_user ID highlight in the image below, and Plaintiff has redacted the corresponding string of numbers to preserve the user's anonymity.

80. When a visitor's browser has recently logged out of an account, Facebook compels the visitor's browser to send a smaller set of cookies.¹⁹

81. The fr cookie contains an encrypted Facebook ID and browser identifier.²⁰ Facebook, at a minimum, uses the fr cookie to identify users, and this particular cookie can stay on a user's website browser for up to 90 days after the user has logged out of Facebook.²¹

82. The cookies listed in the image above are commonly referred to as third-party cookies because they were "created by a website with a domain name other than the one the user is currently visiting"—i.e., Facebook. Although Facebook created these cookies, Defendant is ultimately responsible for the manner in which individual website users were identified via these cookies, and Facebook would not have received this data but for Defendant's implementation and use of the Pixel throughout its website.

83. Defendant also revealed its website visitors' identities via first-party cookies such as the _fbp cookie that Facebook uses to identify a particular browser and a user.²²

84. Importantly, the _fbp cookie is transmitted to Facebook even when the user's browser is configured to block third-party tracking cookies because, unlike the fr cookies and c_user cookie, the _fbp cookie functions as a first-party cookie—i.e. a cookie that was created and placed on the website by Defendant.²³

¹⁹ The screenshot below serves as example and demonstrates the types of data transmitted during an HTTP single communication session. Not pictured here and in the preceding image is the _fbp cookie, which is transmitted as a first-party cookie.

²⁰ Data Protection Commissioner, Facebook Ireland Ltd: Report of Re-Audit (Sept. 21, 2012), p. 33, http://www.europe-v-facebook.org/ODPC_Review.pdf (last visited May 11, 2023).

²¹ Cookies & other storage technologies, FACEBOOK.COM, <https://www.facebook.com/policy/cookies/> (last visited May 11, 2023).

²² *Id.*

²³ The _fbp cookie is always transmitted as a first-party cookie. A duplicate _fbp cookie is

85. The Facebook Tracking Pixel uses both first- and third-party cookies.

86. In summation, Facebook, at a minimum, uses the fr, sb, and c_user cookies to link website visitors' communications and online activity with their corresponding Facebook profiles, and, because the Pixel is automatically programmed to transmit data via both first-party and third-party cookies, patients' information and identities are revealed to Facebook even when they have disabled third-party cookies within their web browsers.

87. At present, the full breadth of Defendant's tracking and data sharing practices is unclear, but other evidence suggests Defendant is using additional tracking pixels and tools to transmit its patients' Private Information to additional third parties. For example, the image below indicates that Defendant is also sending its patients' protected health information to Google via Google Analytics:

sometimes sent as a third-party cookie, depending on whether the browser has recently logged into Facebook.

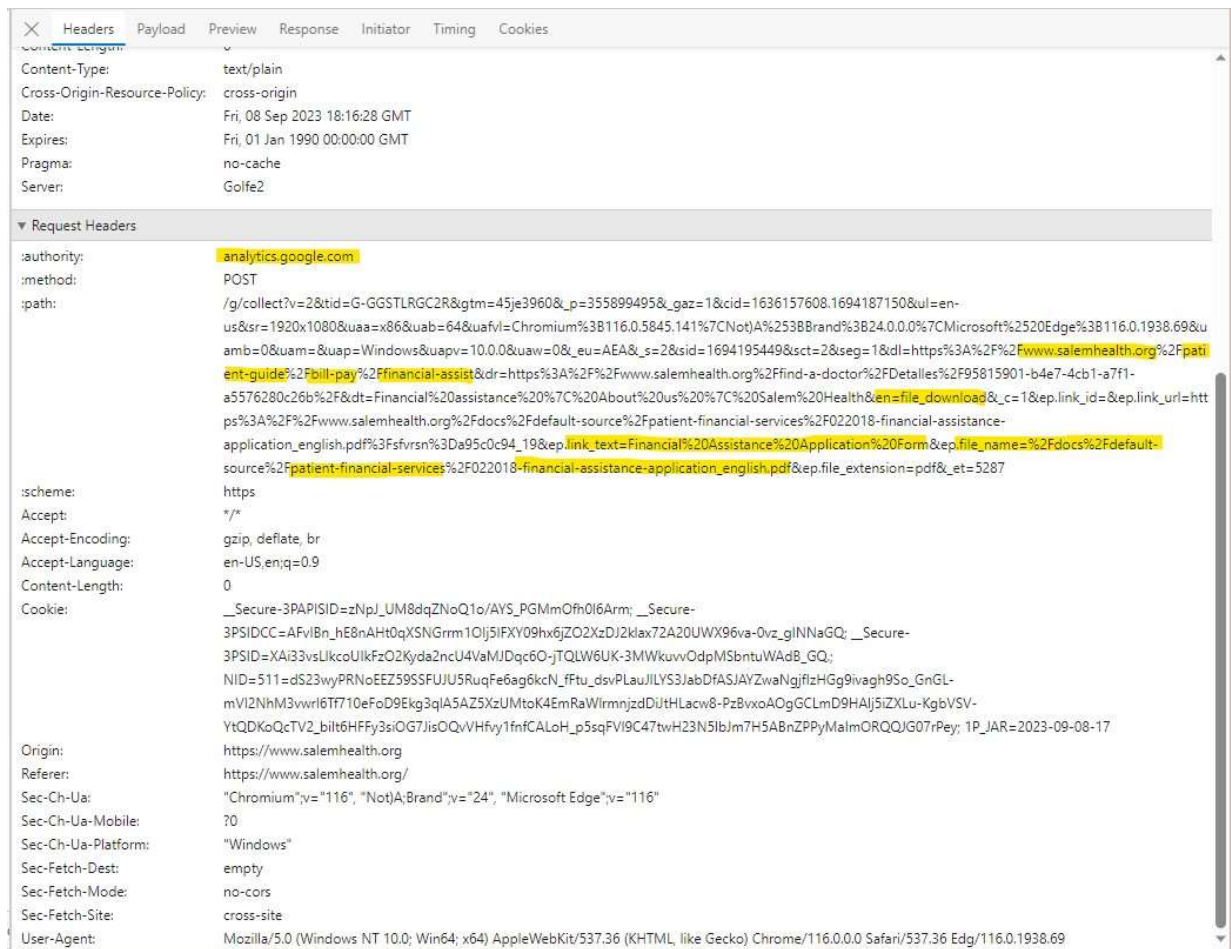


Figure 6. Screenshot of network analysis showing cookies sent to Google when a user fills out a form on salemhealth.org.

88. The image above shows that when a user has completed a form on Defendant's Website to apply for financial assistance related to medical care, the name of the form was sent to Google, thereby revealing the user's status as a patient and that the patient is seeking financial assistance.

89. Defendant does not appear to have enabled the anonymize feature provided by Google Analytics because the text "aip:" does not appear in the image.

90. Accordingly, Google receives patients' communications alongside the patients' IP address, which is also impermissible under HIPAA.

91. Furthermore, Google Analytics was detected on the login page to Defendant's MyChart Portal, enabling Google to identify a particular Website user as a patient of Defendant.

92. Defendant does not disclose that the Pixel, Google Analytics, or any other tracking tools embedded in the Website's source code tracks, records, and transmits Plaintiff's and Class Members' Private Information to Facebook and Google. Moreover, Defendant never received consent or written authorization to disclose Plaintiff's and Class Members' private communications to Facebook or Google.

F. Plaintiff M.R.'s Experience

93. Plaintiff, as Defendant's patient, has received healthcare services from 2006 through the present at hospitals and clinics in Defendant's network and has used Defendant's Website to communicate Private Information to Defendant on numerous occasions.

94. Plaintiff has been a Facebook user since at least 2008.

95. Plaintiff has had a Google account since at least 2019.

96. Plaintiff has been diagnosed with Ehlers-Danlos syndrome, a genetic condition that causes the body's connective tissues to become weaker than they otherwise should be. Ehlers-Danlos syndrome causes joint instability and hypermobility that results in loose, unstable joints that dislocate easily. Additional common symptoms include joint pain and clicking, extreme tiredness or fatigue, and stretchy, fragile skin that bruises easily and does not heal well.

97. Plaintiff also has slipping rib syndrome and costal arch instability, which are independent of but potentially related to her Ehlers-Danlos syndrome.

98. On numerous occasions, Plaintiff accessed Defendant's Website on her computer and/or mobile device for the purpose of finding and obtaining medical treatment for her specific medical conditions. Plaintiff accessed Defendant's Website to receive healthcare services from

Defendant or Defendant's affiliates, at Defendant's direction, and with Defendant's encouragement.

99. Plaintiff has used Defendant's MyChart portal frequently and regularly since 2017 and Defendant's broader Website frequently and regularly since 2019 to research medical symptoms, search for specific doctors and specialists who could help with her specific conditions, make appointments, complete patient web forms, communicate private medical information, check her medical records and test results and upload medical records from other facilities.

100. In particular, Plaintiff has used Defendant's Website to search for neurosurgeons and thoracic surgeons and for information related to Ehlers-Danlos syndrome, slipping rib syndrome, and costal arch instability.

101. Plaintiff communicated with Defendant about her past, present, and future medical care and treatment via the Website. Because Defendant utilized the Facebook Pixel, the Website's Source Code sent a secret set of instructions back to the individual's browser, causing the Pixel to send Plaintiff's FID, the Pixel ID, and both the webpage's and, upon information and belief, MyChart portal's URLs to Facebook.

102. Pursuant to the systematic process described in this Complaint, Plaintiff's Private Information thus was disclosed to Facebook, and this data included her PII, PHI, and related confidential information.

103. In addition, while the Facebook Pixel has been removed from Defendant's Website, the Website still uses the Google Analytics Tracking Tool.²⁴

²⁴ In addition to other pages of the Website, the Google Analytics tool was previously present on Defendant's MyChart portal login page. It has since been removed.

104. Plaintiff searched for information related to Ehlers-Danlos syndrome on Defendant's Website on numerous occasions.

105. As shown in the image below, if a user enters the phrase, "I have Ehlers-Danlos syndrome" into the search bar on Defendant's Website, that exact phrase is sent to Google alongside cookies and device identifiers, thereby revealing the user's identity to Google and allowing it to link the user's specific medical information to the user's identity:

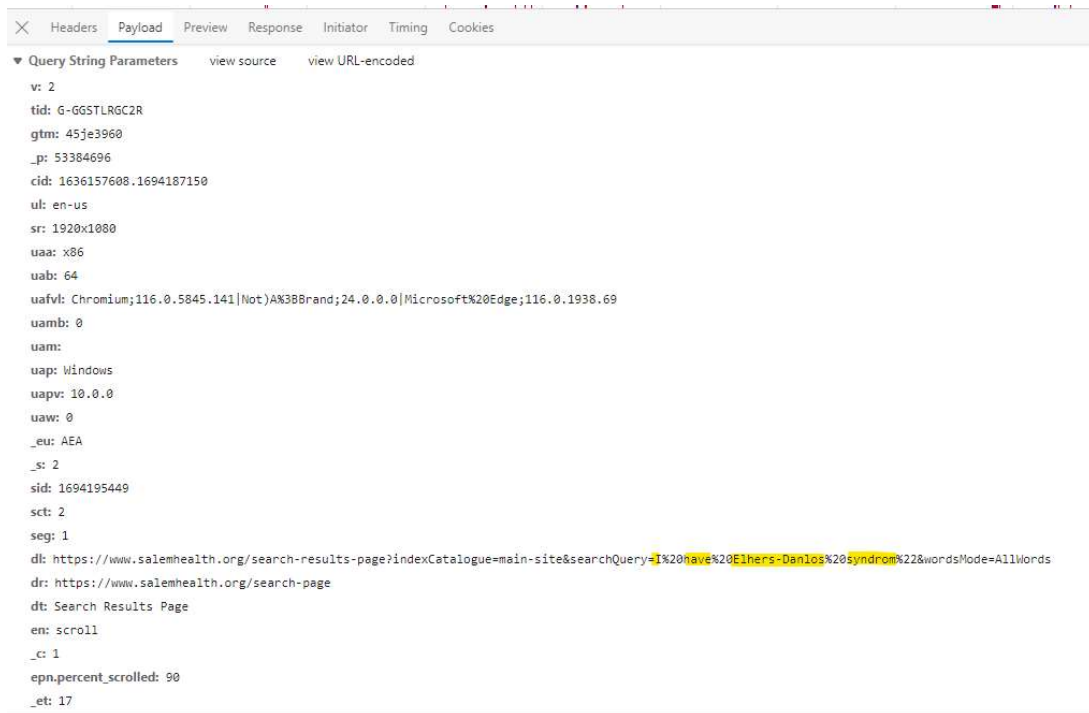


Figure 7. Screenshot of network analysis showing cookies sent to Google when a user uses the search bar on salemhealth.org.

106. Once again, the text "aip:" does not appear in the image, which indicates Defendant has not enabled the anonymize feature provided by Google Analytics and thus the information is individually identifying.

107. Defendant intercepted and/or assisted these interceptions of Plaintiff's communications without Plaintiff's knowledge, consent, or express written authorization. By

failing to receive the requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiff's Private Information.

108. As Defendant's patient, Plaintiff reasonably expected that her online communications with Defendant were solely between herself and Defendant and that such communications would not be transmitted to or disclosed to a third party. But for her status as Defendant's patient, Plaintiff would not have disclosed her Private Information to Defendant.

109. During her time as a patient, Plaintiff never consented to the use of her Private Information by third parties or to Defendant enabling third parties, including Facebook, to access or interpret such information.

110. Notwithstanding, through the Tracking Tools, Defendant transmitted Plaintiff's Private Information to third parties, such as Facebook and Google.

111. During the same transmissions, the Website routinely provides Facebook and Google with its patients' IP addresses, and/or device IDs (and, in the case of Facebook, their FIDs) or other information they input into Defendant's Website, like their home address, zip code, or phone number. This is precisely the type of information that HIPAA requires healthcare providers to anonymize to protect the privacy of patients. Plaintiff's and Class Members identities could be easily determined based on the FID, IP address and/or reverse lookup from the collection of other identifying information that was improperly disclosed.

112. After intercepting and collecting this information, Facebook and Google process it, analyze it, and assimilate it into datasets like Core Audiences and Custom Audiences. If the Website visitor is also a Facebook user, Facebook will associate the information that it collects from the visitor with a Facebook ID that identifies their name and Facebook profile, i.e., their

real-world identity.²⁵ If the patient is a Google user, Google similarly is able to identify the patient.

113. After searching for pain management options on Defendant's Website, Plaintiff observed advertisements on her Facebook account related to pain management medications and treatments.

114. Based on the presence of the Pixel and Conversions API, Defendant unlawfully disclosed Plaintiff's Private Information to Facebook. The presence of Facebook advertisements confirms Defendant's unlawful transmission of Plaintiff's Private Information to Facebook. Said differently, Plaintiff did not disclose this Private Information to any other source—only Defendant's Website.

115. In sum, Defendant's Tracking Tools transmitted Plaintiff's highly sensitive communications and Private Information to Facebook and Google, including communications that contained private and confidential information, without Plaintiff's knowledge, consent, or express written authorization.

116. Plaintiff suffered injuries in the form of (i) invasion of privacy; (ii) diminution of value of the Private Information; (iii) statutory damages; (iv) the continued and ongoing risk to her Private Information; and (v) the continued and ongoing risk of harassment, spam, and targeted advertisements specific to Plaintiff's medical conditions and other confidential information she communicated to Defendant via the Website.

²⁵ A user's Facebook Profile ID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status, and other details. Because the user's Facebook Profile ID uniquely identifies an individual's Facebook account, Meta—or any ordinary person—can easily use the Facebook Profile ID to quickly and easily locate, access, and view the user's corresponding Facebook profile.

117. Plaintiff has a continuing interest in ensuring that future communications with Defendant are protected and safeguarded from future unauthorized disclosure.

G. Defendant’s Conduct Is Unlawful and Violated Industry Norms

i. Defendant Violated HIPAA Standards

118. Under Federal Law, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patients’ express written authorization.²⁶

119. The HIPAA Privacy Rule, located at 45 CFR Part 160 and Subparts A and E of Part 164, “establishes national standards to protect individuals’ medical records and other individually identifiable health information (collectively defined as ‘protected health information’) and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically.”²⁷

120. The Privacy Rule broadly defines “protected health information” (“PHI”) as individually identifiable health information (“IIHI”) that is “transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium.” 45 C.F.R. § 160.103.

121. IIHI is defined as “a subset of health information, including demographic information collected from an individual” that is: (1) “created or received by a health care provider, health plan, employer, or health care clearinghouse”; (2) “[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to

²⁶ HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

²⁷ HHS.gov, HIPAA For Professionals (last visited April 12, 2023), <https://www.hhs.gov/hipaa/forprofessionals/privacy/index.html>.

an individual; or the past, present, or future payment for the provision of health care to an individual”; and (3) either (a) “identifies the individual” or (b) “[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual.” 45 C.F.R. § 160.103.

122. Under the HIPPA de-identification rule, “health information is not individually identifiable only if”: (1) an expert “determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information” and “documents the methods and results of the analysis that justify such determination”; or (2) “the following identifiers of the individual or of relatives, employers, or household members of the individual are removed;

a. Names;

H. Medical record numbers;

J. Account numbers;

M. Device identifiers and serial numbers;

N. Web Universal Resource Locators (URLs);

O. Internet Protocol (IP) address numbers; ... and

R. Any other unique identifying number, characteristic, or code...;and”

The covered entity must not “have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.”

45 C.F.R. § 160.514.

123. The HIPAA Privacy Rule requires any “covered entity”—which includes health care providers—to maintain appropriate safeguards to protect the privacy of protected health

Page 31 – CLASS ACTION ALLEGATION COMPLAINT

information and sets limits and conditions on the uses and disclosures that may be made of protected health information without authorization. 45 C.F.R. §§ 160.103, 164.502.

124. An individual or corporation violates the HIPAA Privacy Rule if it knowingly and in violation of 42 U.S.C. §§ 1320d-1320d-9 (“Part C”): “(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual.” The statute states that a “person ... shall be considered to have obtained or disclosed individually identifiable health information in violation of [Part C] if the information is maintained by a covered entity ... and the individual obtained or disclosed such information without authorization.” 42 U.S.C. § 1320d-6.

125. The criminal and civil penalties imposed by 42 U.S.C. § 1320d-6 apply directly to Defendant when it is knowingly disclosing individually identifiable health information relating to an individual, as those terms are defined under HIPAA.

126. Violation of 42 U.S.C. § 1320d-6 is subject to criminal penalties. 42 U.S.C. § 1320d-6(b). There is a penalty enhancement where “the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm.” In such cases, the entity that knowingly obtains individually identifiable health information relating to an individual shall “be fined not more than \$250,000, imprisoned not more than 10 years, or both.”

127. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the HHS instructs:

Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a

phone book, then this information would not be PHI because it is not related to health data... If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.²⁸

128. In its guidance for Marketing, the HHS further instructs:

The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. ... Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, *covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list.* (Emphasis added).²⁹

129. As alleged above, there is an HHS Bulletin that highlights the obligations of "regulated entities," which are HIPAA-covered entities and business associates, when using tracking technologies.³⁰

130. The Bulletin expressly provides that "[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules."

131. Defendant's actions violated HIPAA Rules per this Bulletin.

ii. Defendant Violated Oregon Law

132. Oregon law has established policies and procedures for the maintenance, preservation, and storage of patient medical records.

²⁸https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (last visited Nov. 3, 2022).

²⁹<https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf> (last visited Nov. 3, 2022)

³⁰ See <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>.

133. Oregon law provides that “(1) It is the policy of the State of Oregon that an individual has:(a) The right to have protected health information of the individual safeguarded from unlawful use or disclosure.” Or. Rev. Stat. Ann. § 192.553.

134. Oregon law also provides in Or. Rev. Stat. Ann. § 192.558 that PHI may only be used or disclosed consistent with prior authorization or without such authorization in particular circumstances.

135. Defendant’s disclosure of PHI by use of Tracking Technologies does not fit within any prior authorization or circumstances provided in Or. Rev. Stat. Ann. § 192.558.

136. Defendant’s actions described herein violated Oregon law.

iii. Defendant Violated Industry Standards

137. A medical provider’s duty of confidentiality is a cardinal rule and is embedded in the physician-patient and hospital-patient relationship.

138. The American Medical Association’s (“AMA”) Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

139. AMA Code of Ethics Opinion 3.1.1 provides:

Protecting information gathered in association with the care of the patient is a core value in health care... Patient privacy encompasses a number of aspects, including, ... personal data (informational privacy)

140. AMA Code of Medical Ethics Opinion 3.2.4 provides:

Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (A) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient’s authorized

surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

141. AMA Code of Medical Ethics Opinion 3.3.2 provides:

Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically...must...(c) release patient information only in keeping ethics guidelines for confidentiality.

H. Plaintiff's and Class Members' Expectation of Privacy

142. Plaintiff and Class Members were aware of Defendant's duty of confidentiality when they sought medical services from Defendant.

143. Indeed, at all times when Plaintiff and Class Members provided their Private Information to Defendant, they all had a reasonable expectation that the information would remain private and that Defendant would not share the Private Information with third parties for a commercial purpose, unrelated to patient care.

144. Plaintiff and Class Members would not have used Defendant's Website, would not have provided their Private Information to Defendant, and would not have paid for Defendant's healthcare services, or would have paid less for them, had they known that Defendant would disclose their Private Information to third parties.

I. IP Addresses Are PII

145. On information and belief, through the use of the Tracking Tools on Defendant's Website, Defendant also disclosed and otherwise assisted third parties with intercepting Plaintiff's and Class Members' Computer IP addresses.

146. An IP address is a number that identifies the address of a device connected to the Internet.

147. IP addresses are used to identify and route communications on the Internet.

148. IP addresses of individual Internet users are used by Internet service providers, websites, and third-party tracking companies to facilitate and track Internet communications.

149. Facebook tracks every IP address ever associated with a Facebook user.

150. Facebook tracks IP addresses for use of targeting individual homes and their occupants with advertising.

151. As to Google, over 70% of online websites use Google's visitor-tracking products, Google Analytics and Google Ad Manager.

152. Whenever a user visits a website that is running Google Analytics and Google Ad Manager, Google's software scripts on the website surreptitiously direct the user's browser to send a secret, separate message to Google's servers in California, which includes the user's IP address, the user's geolocation, information contained in Google cookies, any user-ID issued by the website to the user, and information about the browser the user is using.

153. Under HIPAA, an IP address is considered PII:

- HIPAA defines PII to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses. *See* 45 C.F.R. § 164.514 (2).
- HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *See also*, 45 C.F.R. § 164.514(b)(2)(i)(O).

154. Consequently, by disclosing IP addresses, Defendant's business practices violated HIPAA and industry privacy standards.

J. Defendant Was Enriched and Benefitted from the Use of The Tracking Tools and Unauthorized Disclosures

155. The primary motivation and a determining factor in Defendant's interception and disclosure of Plaintiff's and Class Members' Private Information was to commit criminal and tortious acts in violation of federal and state laws as alleged herein, namely, the use of patient data for advertising in the absence of express written consent. Defendant's further use of the Private Information after the initial interception and disclosure for marketing and revenue generation was in violation of HIPAA and an invasion of privacy. In exchange for disclosing the Private Information of its patients, Defendant is compensated by Facebook in the form of enhanced advertising services and more cost-efficient marketing on its platform.

156. Retargeting is a form of online marketing that targets users with ads based on their previous internet communications and interactions.

157. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients to get more patients to use its services. Defendant did so through use of the intercepted patient data it obtained, procured, and/or disclosed in the absence of express written consent.

158. By utilizing the Tracking Tools, the cost of advertising and retargeting was reduced through further use of the unlawfully intercepted and disclosed Private Information, thereby benefitting Defendant while invading the privacy of Plaintiff and Class Members and violating their rights under federal and Oregon law.

K. Plaintiff's and Class Members' Private Information Had Financial Value

159. Plaintiff's data and Private Information has economic value. Facebook regularly uses data that it acquires to create Core and Custom Audiences, as well as Lookalike Audiences

and then sells that information to advertising clients. Google has recognized the value of user data and has even instituted a pilot program in which it pays users \$3 per week to track them online.

160. Data harvesting is one of the fastest growing industries in the country, and consumer data is so valuable that it has been described as the “new oil.” Conservative estimates suggest that in 2018, Internet companies earned \$202 per American user from mining and selling data. That figure is only due to keep increasing; estimates for 2022 are as high as \$434 per user, for a total of more than \$200 billion industry wide.

161. The value of health data in particular is well-known and has been reported on extensively in the media. For example, Time Magazine published an article in 2017 titled “How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry” in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.³¹

162. Similarly, CNBC published an article in 2019 in which it observed that “[d]e-identified patient data has become its own small economy: There’s a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers.”³²

163. Indeed, numerous marketing services and consultants offering advice to companies on how to build their email and mobile phone lists—including those seeking to take advantage of targeted marketing—direct putative advertisers to offer consumers something of

³¹ See <https://time.com/4588104/medical-data-industry/> (last visited February 16, 2023).

³² See <https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html> (last visited March 1, 2023).

value in exchange for their personal information. “No one is giving away their email address for free. Be prepared to offer a book, guide, webinar, course or something else valuable.”³³

164. There is also a market for data in which consumers can participate. Personal information has been recognized by courts as extremely valuable. *See In re Marriott Int’l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) (“Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.”).

165. Several companies have products through which they pay consumers for a license to track their data. Google, Nielsen, UpVoice, HoneyGain, and SavvyConnect are all companies that pay for browsing historical information.

166. Facebook also has paid users for their digital information, including browsing history. Until 2019, Facebook ran a “Facebook Research” app through which it paid \$20 a month for a license to collect browsing history information and other communications from consumers between the ages 13 and 35.

167. Additionally, healthcare data is extremely valuable to bad actors. Health care records may be valued at up to \$250 per record on the black market.³⁴

³³ VERO, HOW TO COLLECT EMAILS ADDRESSES ON TWITTER <https://www.getvero.com/resources/twitter-lead-generation-cards/>. (last visited Sep. 1, 2023).

³⁴ Tori Taylor, *Hackers, Breaches, and the Value of Healthcare Data*, *SecureLink* (June 30, 2021), <https://www.securelink.com/blog/healthcare-data-new-prize-hackers>.

TOLLING

168. Any applicable statute of limitations has been tolled by the “delayed discovery” rule. Plaintiff did not know (and had no way of knowing) that her PII and PHI was intercepted and unlawfully disclosed to Facebook because Defendant kept this information secret.

CLASS ACTION ALLEGATIONS

169. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated (“the Class”) pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

170. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

All individuals residing in the United States who are, or were, patients of Defendant or any of its affiliates, used Defendant’s Website, and had their Private Information disclosed to a third party without authorization.

In the alternative, Plaintiff seeks to represent an “Oregon Class” defined as:

All individuals residing in Oregon who are, or were, patients of Defendant or any of its affiliates, used Defendant’s Website, and had their Private Information disclosed to a third party without authorization or consent.

The Nationwide Class and Oregon Class are collectively referred to as the “Class.”

171. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

172. Plaintiff reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

173. Numerosity, Fed R. Civ. P. 23(a)(1). The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are hundreds of

thousands of individuals whose PII and PHI may have been improperly disclosed to Facebook, and the Class is identifiable within Defendant's records.

174. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3). Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

- a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class Members;
- b. Whether Defendant had duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;
- c. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information would be disclosed to third parties;
- d. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;
- e. Whether Defendant adequately addressed and fixed the practices which permitted the disclosure of patient Private Information;
- f. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;
- g. Whether Defendant's conduct violated the Oregon's Policy for Protected Health Information, Or. Rev. Stat. Ann. § 192.553, *et seq.*
- h. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct; and

- i. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of Defendant's disclosure of their Private Information.

175. Typicality, Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of Defendant's incorporation of the Facebook Pixel, due to Defendant's misfeasance.

176. Adequacy, Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

177. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3). Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against a large corporation like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

178. Policies Generally Applicable to the Class. Fed. R. Civ. P. 23(b)(2). This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

179. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

180. The litigation of the claims is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

181. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

182. Unless a class-wide injunction is issued, Defendant may continue disclosing the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the practices complained of herein, and Defendant may continue to act unlawfully as set forth in this Complaint.

183. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

184. Issue Certification, Fed. R. Civ. P. 23(c)(4). Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to, the following:

- a. Whether Defendant owed a legal duty to not disclose Plaintiff's and Class Members' Private Information;
- b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;
- c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
- d. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information would be disclosed to third parties;

- e. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties;
- f. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the Class)

185. Plaintiff incorporates all prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

186. Medical providers have a duty to their patients to keep non-public medical information completely confidential, and to safeguard sensitive personal and medical information. This duty arises from the implied covenant of trust and confidence that is inherent in the physician-patient relationship.

187. Medical providers also have a duty to maintain the confidentiality of Plaintiff's PHI under HIPAA and its implementing regulations, as well as Oregon state law governing PHI, Or. Rev. Stat. Ann. §§ 192.553 to 192.581.

188. Plaintiff and Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Website.

189. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became a guardian of Plaintiff's and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its patients, including Plaintiff and Class

Members: (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of disclosure of their Private Information to unauthorized third parties; and (3) to maintain complete and accurate records of what patient information (and where) Defendant did and does store and disclose.

190. Contrary to its duties as a medical provider and its express and implied promises of confidentiality, Defendant installed its Tracking Tools to disclose and transmit to third parties Plaintiff's and Class Members' communications with Defendant as well as the contents of those communications, including Private Information.

191. These disclosures were made for commercial purposes without Plaintiff's or Class Members' knowledge, consent, or authorization, and were unprivileged.

192. The unauthorized disclosures of Plaintiff's and Class Members' Private Information were intentionally caused by Defendant's employees acting within the scope of their employment. Alternatively, the disclosures of Plaintiff's and Class Members' Private Information occurred because of Defendant's negligent hiring or supervision of its employees or agents, its failure to establish adequate policies and procedures to safeguard the confidentiality of patient information, or its failure to train its employees or agents to properly discharge their duties under those policies and procedures.

193. The third-party recipients included, but may not be limited to, Facebook and Google. Such information was received by these third parties in a manner that allowed them to identify the Plaintiff and the individual Class Members.

194. Defendant's breach of the common law implied covenant of trust and confidence is further evidenced by its failure to comply with federal and state privacy regulations, including:

- a. By failing to ensure the confidentiality and integrity of electronic PHI Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1);
- b. By failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- c. By failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(4);
- d. By failing to obtain satisfactory assurances, including in writing, that its business associates and/or subcontractors would appropriately safeguard Plaintiff's and Class Members PHI;
- e. By failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);
- f. By failing to implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network in violation of 45 C.F.R. § 164.312(e)(1);
- g. By impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, *et seq.*;
- h. By failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5);
- i. By failing to keep Private Information confidential as required by Or. Rev. Stat. Ann. § 192.553, *et seq.*; and
- j. By otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

195. The harm arising from a breach of provider-patient confidentiality includes mental suffering due to the exposure of private information and erosion of the essential confidential relationship between the healthcare provider and the patient.

196. As a direct and proximate cause of Defendant's unauthorized disclosures of patient personally identifiable, non-public medical information, and communications, Plaintiff and Class members were damaged by Defendant's breach in that:

- a. Sensitive and confidential information that Plaintiff and Class members intended to remain private is no longer private;
- b. Plaintiff and Class members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements;
- c. Defendant eroded the essential confidential nature of the provider-patient relationship;
- d. General damages for invasion of their rights in an amount to be determined by a jury;
- e. Nominal damages for each independent violation;
- f. Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without compensation for such data;
- g. Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;
- h. Defendant's actions diminished the value of Plaintiff's and Class Members' Private Information; and
- i. Defendant's actions violated the property rights Plaintiff and Class members have in their Private Information.

COUNT II
VIOLATION OF ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA")
18 U.S.C. § 2511(1) *et seq.*
UNAUTHORIZED INTERCEPTION, USE, AND DISCLOSURE
(On Behalf of Plaintiff and the Class)

197. Plaintiff incorporates the prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

198. The ECPA protects both sending and receipt of communications.

199. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

200. The transmissions of Plaintiff's Private Information to Defendant via Defendant's Website qualifies as a "communication" under the ECPA's definition in 18 U.S.C. § 2510(12).

201. The transmissions of Plaintiff's Private Information to medical professionals qualifies as a "communication" under the ECPA's definition in 18 U.S.C. § 2510(2).

202. **Electronic Communications.** The transmission of Private Information between Plaintiff and Class Members and Defendant via its Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing,...data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

203. **Content.** The ECPA defines content, when used with respect to electronic communications, to "include[] *any* information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (emphasis added).

204. **Interception.** The ECPA defines the interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents ... include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

205. **Electronic, Mechanical, or Other Device.** The ECPA defines "electronic, mechanical, or other device" as "any device ... which can be used to intercept a[n] ... electronic

communication[.]” 18 U.S.C. § 2510(5). The following constitute “devices” within the meaning of 18 U.S.C. § 2510(5):

- a. Plaintiff’s and Class Members’ browsers;
- b. Plaintiff’s and Class Members’ computing devices;
- c. Defendant’s web-servers; and
- d. The Pixel deployed by Defendant to effectuate the sending and acquisition of patient communications

206. Whenever Plaintiff and Class Members interacted with Defendant’s Website, Defendant, through the Tracking Tools embedded and operating on its Website, contemporaneously and intentionally disclosed, and endeavored to disclose the contents of Plaintiff’s and Class Members’ electronic communications to third parties, including Facebook and Google, without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C. § 2511(1)(c).

207. Whenever Plaintiff and Class Members interacted with Defendant’s Website, Defendant, through the Tracking Tools embedded and operating on its Website, contemporaneously and intentionally used, and endeavored to use the contents of Plaintiff’s and Class Members’ electronic communications, for purposes other than providing health care services to Plaintiff and Class Members without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C. § 2511(1)(d).

208. Whenever Plaintiff and Class Members interacted with Defendant’s Website, Defendant, through the Tracking Tools it embedded and operated on its Website, contemporaneously and intentionally redirected the contents of Plaintiff’s and Class Members’

electronic communications while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication, including Facebook and Google.

209. Defendant's intercepted communications include, but are not limited to, the contents of communications to/from Plaintiff's and Class Members' regarding PII and PHI, treatment, medication, and scheduling.

210. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiff and Class Members to affiliates and other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

211. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiff and Class Members, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

212. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the Tracking Tools to track and utilize Plaintiff's and Class Members' PII and PHI for financial gain.

213. Defendant was not acting under color of law to intercept Plaintiff's and Class Members' wire or electronic communication.

214. Plaintiff and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiff's privacy via the Pixel tracking code.

215. Any purported consent that Defendant received from Plaintiff and Class Members was not valid.

216. **Unauthorized Purpose.** Defendant intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a tortious or criminal act in violation of the Constitution or laws of the United States or of any State – namely, violations of HIPAA, the Oregon's Protected Health Information Policy, and invasion of privacy, among others.

217. The ECPA provides that a “party to the communication” may be liable where a “communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.” 18 U.S.C § 2511(2)(d).

218. Defendant is a “party to the communication” with respect to patient communications. However, Defendant's simultaneous, unknown duplication, forwarding, and interception of Plaintiff's and Class Members' Private Information does not qualify for the party exemption.

219. Defendant's acquisition of patient communications that were used and disclosed to Facebook and Google was done for purposes of committing criminal and tortious acts in violation of the laws of the United States and Oregon, including.

- a. Criminal violation of HIPAA, 42 U.S.C. § 1320d-6; ‘
- b. Oregon's Protected Health Information Policy, Or. Rev. Stat. Ann. § 192.553, *et seq*;
- c. Invasion of Privacy; and
- d. Breach of Contract.

220. Under 42 U.S.C. § 1320d-6, it is a criminal violation for a person to “use[] or cause[] to be used a unique health identifier” or to “disclose[] individually identifiable health information to another person ... without authorization” from the patient.

221. The penalty for violation is enhanced where “the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm.” 42 U.S.C. § 1320d-6.

222. Defendant’s conduct violated 42 U.S.C. § 1320d-6 in that it:

- a. Used and caused to be used cookie identifiers associated with specific patients without patient authorization; and
- b. Disclosed individually identifiable health information to Facebook and Google without patient authorization.

223. Defendant’s conduct would be subject to the enhanced provisions of 42 U.S.C. § 1320d-6 because Defendant’s use of the Facebook and Google source code was for Defendant’s commercial advantage to increase revenue from existing patients and gain new patients.

224. The fbp, ga, and gid cookies, which constitute programs, commanded Plaintiffs’ and Class Members’ computing devices to remove and redirect their data and the content of their communications with Defendant to Google, Facebook, and others.

225. Defendant knew or had reason to know that the fbp, ga, and gid cookies would command Plaintiffs’ and Class Members’ computing devices to remove and redirect their data and the content of their communications with Defendant to Google, Facebook, and others.

226. Defendant is not exempt from ECPA liability under 18 U.S.C. § 2511(2)(d) on the ground that it was a participant in Plaintiffs’ and Class Members’ communications about their individually-identifiable patient health information on its Website, because it used its

participation in these communications to improperly share Plaintiff's and Class Members' individually-identifiable patient health information with Facebook and Google, third-parties that did not participate in these communications, that Plaintiff and Class Members did not know were receiving their individually-identifiable patient health information, and that Plaintiff and Class Members did not consent to receive this information.

227. Defendant accessed, obtained, and disclosed Plaintiff's and Class Members' Private Information for the purpose of committing the crimes and torts described herein because it would not have been able to obtain the information or the marketing services if it had complied with the law.

228. As such, Defendants cannot viably claim any exception to ECPA liability.

229. Plaintiff and Class Members have suffered damages as a direct and proximate result of Defendant's invasion of privacy in that:

- a. Learning that Defendant has intruded upon, intercepted, transmitted, shared, and used their individually-identifiable patient health information (including information about their medical symptoms, conditions, and concerns, medical appointments, healthcare providers and locations, medications and treatments, and health insurance and medical bills) for commercial purposes has caused Plaintiff and the Class Members to suffer emotional distress;
- b. Defendant received substantial financial benefits from its use of Plaintiff's and Class Members' individually-identifiable patient health information without providing any value or benefit to Plaintiff or the Class Members;
- c. Defendant received substantial, quantifiable value from its use of Plaintiff's and Class Members' individually-identifiable patient health information, such as understanding

how people use its website and determining what ads people see on its website, without providing any value or benefit to Plaintiffs or the Class Members;

- d. Defendant has failed to provide Plaintiff and the Class Members with the full value of the medical services for which they paid, which included a duty to maintain the confidentiality of their patient information; and
- e. The diminution in value of Plaintiffs' and Class Members' PII and PHI and the loss of privacy due to Defendant making sensitive and confidential information, such as patient status, test results, and appointments that Plaintiffs and Class Members intended to remain private no longer private.

230. As a result of Defendant's violation of the ECPA, Plaintiff and Class Members are entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of \$100 a day for each day of violation or \$10,000, equitable or declaratory relief, compensatory and punitive damages, and attorney's fees and costs.

COUNT III
INVASION OF PRIVACY
(Intrusion upon Seclusion)
(On Behalf of Plaintiff and the Class)

231. Plaintiff incorporates the prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

232. The Private Information of Plaintiff and Class Members consists of private and confidential facts and information that were never intended to be shared beyond private communications.

233. Plaintiff and Class Members had a legitimate expectation of privacy regarding their Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

234. Defendant owed a duty to Plaintiff and Class Members to keep their Private Information confidential.

235. Defendant owed a duty to Plaintiff and Class Members not to give publicity to their private lives to Facebook and Google and, by extension, other third-party advertisers and businesses who purchased Facebook's and Google's advertising services.

236. Defendant's unauthorized disclosure of Plaintiff's and Class Members' Private Information to Facebook and Google, third-party social media and marketing giants, is highly offensive to a reasonable person.

237. Defendant's willful and intentional disclosure of Plaintiff's and Class Members' Private Information constitutes an intentional interference with Plaintiff's and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

238. Defendant's conduct constitutes an intentional physical or sensory intrusion on Plaintiff's and Class Members' privacy because Defendant exceeded its authorization to access Plaintiff's and Class Members' information and facilitated Facebook's and Google's simultaneous eavesdropping and wiretapping of confidential communications.

239. Defendant failed to protect Plaintiff's and Class Members' Private Information and acted knowingly when it installed the Tracking Tools onto its Website because the purpose of the Tracking Tools is to track and disseminate individual's communications with the Website for the purpose of marketing and advertising.

240. Because Defendant intentionally and willfully incorporated the Tracking Tools into its Website and encouraged patients to use that Website for healthcare purposes, Defendant had notice and knew that its practices would cause injury to Plaintiff and Class Members.

241. As a proximate result of Defendant's acts and omissions, the private and sensitive PII and PHI of Plaintiff and the Class Members was disclosed to third parties without authorization, causing Plaintiff and the Class to suffer damages.

242. Plaintiff, on behalf of herself and Class Members, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, loss of time and opportunity costs, plus prejudgment interest, and costs.

243. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their Private Information is still maintained by Defendant and still in the possession of Facebook, Google, and other third parties and the wrongful disclosure of the information cannot be undone.

244. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not undo Defendant's disclosure of the information to Facebook and Google who, on information and belief, continue to possess and utilize that information.

245. Plaintiff, on behalf of herself and Class Members, further seeks injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff's and Class Members' Private Information and to adhere to its common law, contractual, statutory, and regulatory duties.

COUNT IV
BREACH OF IMPLIED CONTRACT
(on behalf of Plaintiff and the Class)

246. Plaintiff incorporates the prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

247. As a condition of utilizing Defendant's Website and receiving services from Defendant's healthcare facilities and professionals, Plaintiff and the Class Members provided their Private Information and compensation for their medical care.

248. When Plaintiff and Class Members provided their Private Information to Defendant, they entered into an implied contract pursuant to which Defendant agreed to safeguard and not disclose their Private Information without consent.

249. Plaintiff and Class Members would not have entrusted Defendant with their Private Information in the absence of an implied contract between them and Defendant obligating Defendant to not disclose Private Information without consent.

250. Plaintiff and Class Members would not have retained Defendant to provide healthcare services in the absence of an implied contract between them and Defendant obligating Defendant to not disclose Private Information without consent.

251. Defendant breached these implied contracts by disclosing Plaintiff's and Class Members' Private Information without consent to third parties like Facebook or Google.

252. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiff and Class Members sustained damages as alleged herein, including but not limited to the loss of the benefit of their bargain and diminution in value of Private Information.

253. Plaintiff and Class Members are entitled to compensatory and consequential damages as a result of Defendant's breach of implied contract.

COUNT V
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Class)

254. Plaintiff incorporates the prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

255. Defendant benefits from the use of Plaintiff's and Class Members' Private Information and unjustly retained those benefits at their expense.

256. Plaintiff and Class Members conferred a benefit upon Defendant in the form of Private Information that Defendant collected from Plaintiff and Class Members, without authorization and proper compensation to exceed the limited authorization and access to that information which was given to Defendant.

257. Defendant exceeded any authorization given and instead consciously disclosed and used this information for its own gain, providing Defendant with economic, intangible, and other benefits, including substantial monetary compensation.

258. Defendant unjustly retained those benefits at the expense of Plaintiff and Class Members because Defendant's conduct damaged Plaintiff and Class Members, all without providing any commensurate compensation to Plaintiff and Class Members.

259. The benefits that Defendant derived from Plaintiff and Class Members was not offered by Plaintiff and Class Members gratuitously and rightly belongs to Plaintiff and Class Members. It would be against equity and good conscience for Defendant to be permitted to retain any of the profit or other benefits wrongly derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

260. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds that Defendant received, and such other relief as the Court may deem just and proper.

COUNT VI
NEGLIGENCE
(On behalf of Plaintiff and the Class)

261. Plaintiff incorporates the prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

262. Defendant owed Plaintiff and Class Members a duty to keep their Private Information completely confidential, and to safeguard sensitive personal and medical information.

263. Plaintiff and Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Website.

264. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant installed its Tracking Tools to disclose and transmit to third parties Plaintiff's and Class Members' communications with Defendant, including Private Information and the contents of such information.

265. These disclosures were made without Plaintiff's or Class Members' knowledge, consent, or authorization, and were unprivileged.

266. The third-party recipients included, but may not be limited to, Facebook and/or Google.

267. As a direct and proximate cause of Defendant's unauthorized disclosures of patient personally identifiable, non-public medical information, and communications, Plaintiff and Class members were damaged by Defendant's breach in that:

- a. Sensitive and confidential information that Plaintiff and Class members intended to remain private is no longer private;
- b. Plaintiff and Class members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements;
- c. Defendant eroded the essential confidential nature of the provider-patient relationship;
- d. General damages for invasion of their rights in an amount to be determined by a jury;
- e. Nominal damages for each independent violation;
- f. Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without compensation for such data;
- g. Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;
- h. Defendant's actions diminished the value of Plaintiff's and Class Members' Private Information; and
- i. Defendant's actions violated the property rights Plaintiff and Class Members have in their Private Information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court grant the following:

- A. For an Order certifying the Class and appointing Plaintiff and Counsel to represent such Class;

- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct alleged in this Complaint pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members;
- C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members:
- D. For an award of damages, including, but not limited to, actual, consequential, statutory, punitive, and nominal damages, as allowed by law in an amount to be determined;
- E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- F. For prejudgment interest on all amounts awarded; and
- G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

DATED this 15th day of November, 2023.

STOLL STOLL BERNE LOKTING
& SHLACHTER P.C.

By: s/Timothy S. DeJong
Timothy S. DeJong, OSB No. 940662

209 SW Oak Street, Suite 500
Portland, OR 97204
Telephone: (503) 227-1600
Facsimile: (503) 227-6840
Email: tdejong@stollberne.com

-AND-

Gary M. Klinger*
**MILBERG COLEMAN BRYSON PHILLIPS
GROSSMAN, PLLC**
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
Email: gklinger@milberg.com

Glen L. Abramson*
Alexandra M. Honeycutt
**MILBERG COLEMAN BRYSON PHILLIPS
GROSSMAN, PLLC**
800 S. Gay Street, Suite 1100
Knoxville, TN 37929
Telephone: (866) 252-0878
Email: gabramson@milberg.com
ahoneycutt@milberg.com

Bryan L. Bleichner*
Philip J. Krzeski*
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300
Facsimile: (612) 336-2940
Email: bbleichner@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

Terence R. Coates*
Dylan J. Gould*
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court St., Ste. 530
Cincinnati, Ohio 4502
Telephone: (513) 651-3700
Facsimile: (513) 665-0219
Email: tcoates@msdlegal.com
dgould@msdlegal.com

Joseph M. Lyon*
THE LYON FIRM
2754 Erie Ave.
Cincinnati, Ohio 45208
Telephone: (513) 381-2333
Facsimile: (513) 766-9011
Email: jlyon@thelyonfirm.com

Counsel for Plaintiff

* *pro hac vice* application forthcoming